CLAIMS:

1. An electronic voting method comprising the step of using a fair blind signature scheme to obtain a digital signature (y_i) of a data signal (x_i) comprising a voter's vote (v_i).

2. The electronic voting method of claim 1, wherein the fair blind signature scheme is a threshold fair blind signature scheme in which the digital signature is obtained from a sub-set of a group of servers, the group of servers containing n servers and the sub-set containing t servers, where $t < n$.

3. The electronic voting method of claim 1 or 2, wherein the data signal (x_i) corresponds to the voter's vote (v_i) encrypted according to a first encryption scheme ($\mathcal{E}_{TM}$), said first encryption scheme being the encryption scheme of a first mix-net (TM), and the method further comprises the step of applying the decryption scheme ($\mathcal{D}_{TM}$) inverse to said first encryption scheme to said data signal (x_i) whereby to retrieve the voter's vote (v_i).

4. The electronic voting method of claim 3, and comprising the steps of:

receiving, in a first order, a batch of encrypted data signals, each encrypted data signal (c_i) comprising data encrypted according to a second encryption scheme ($\mathcal{E}_M$) said data including a respective data signal (x_i);

retrieving each data signal (x_i) from the respective encrypted data signal (c_i) in said batch by applying a decryption scheme ($\mathcal{D}_M$) inverse to said second encryption scheme ($\mathcal{E}_M$); and

outputting the retrieved data signals (x_i) for said batch in a different order from said first order.

5. The electronic voting method of claim 4, wherein said second encryption scheme is the encryption scheme of a second mix-net ($\mathcal{M}$).

6. The electronic voting method of claim 5, and comprising the step of detecting irregularities in the voting process, said step of detecting irregularities comprising verifying that the ballots to be counted do not contain duplicated data-pairs, wherein a data-pair corresponds to one of said data signals and the digital signature thereof.

7. The electronic voting method of claim 5, and comprising the step of detecting irregularities in the voting process, wherein the step of detecting irregularities comprises checking the validity of the digital signatures in the ballots to be counted.

8. The electronic voting method of claim 5, and comprising the step of detecting irregularities in the voting process, wherein the step of detecting irregularities comprises checking that there is no overlap between the ballots to be counted and entries in a revocation list

9. An electronic voting method according to any previous claim and comprising the steps of:

receiving said data signal (x_i) for digital signature according to said fair blind signature scheme at a server module ($\mathcal{AS}$), said data signal (x_i) comprising a vote (v_i) selected by a voter ($\mathcal{V}_i$), said vote (v_i) being encrypted according to said first encryption scheme ($\mathcal{E}_{TM}$), blinded according to said fair blind signature scheme and digitally signed according to a digital signature scheme of said voter;

verifying, by said server module ($\mathcal{AS}$), that the digital signature (s_i) in the received signal is valid;

in the case where the verifying step confirms that the digital signature in the signal received by said server module ($\mathcal{AS}$) is valid, said server module

($\mathcal{AS}$) digitally signs the blinded encrypted vote (e_i) and outputs the digitally-signed message ($S_{\mathcal{AS}}(e_i)$);

unblinding the digitally-signed message ($S_{\mathcal{AS}}(e_i)$) to yield said digital signature (y_i) of the data signal (x_i);

encrypting said data signal (x_i) and said digital signature (y_i) thereof according to said second encryption scheme ($\mathcal{E}_{\mathcal{M}}$) to produce encrypted data signal (c_i); and

signing said encrypted data signal according to a signature scheme of the voter ($\mathcal{V}_i$).

10. An electronic voting system comprising:
a plurality of voter modules (10), and
an admin server module (20),
wherein a voter module (10) and the admin server module (20) cooperate in application of a fair blind signature scheme whereby to obtain a digital signature (y_i) of a data signal (x_i) comprising the respective voter's vote (v_i).

11. A voter module (10) adapted to cooperate with an admin server module (20) in application of a fair blind signature scheme whereby to obtain a digital signature (y_i) of a data signal (x_i) comprising the voter's vote (v_i).

12. A computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voter module (10) according to claim 11.

13. A voting system admin server module (20) adapted to cooperate with a voter module (10) in application of a fair blind signature scheme whereby to obtain a digital signature (y_i) of a data signal (x_i) comprising the voter's vote (v_i).

14. A computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system admin server module (20) according to claim 13.

15. A voting system randomizer module (40) comprising:

input means for receiving a batch of cast votes, each cast vote comprising an encrypted data signal (c_i) comprising a respective voter's vote (v_i) digitally signed according to a fair blind signature scheme, each encrypted data signal (c_i) being encrypted according to a predetermined encryption scheme ($\mathcal{E}_M$); and

a mix-net ($\mathcal{M}$) for decrypting said encrypted data signals (c_i) by applying a decryption scheme ($\mathcal{D}_M$) inverse to said predetermined encryption scheme ($\mathcal{E}_M$); and

output means for outputting the decrypted signals of said batch in an order different from the order of the corresponding encrypted data signals in said batch.

16. A computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system randomizer module (40) according to claim 15.

17. A voting system tallier module (50) comprising:

input means for receiving cast votes, each cast vote comprising a data signal (x_i) digitally signed according to a fair blind signature scheme, each data signal (x_i) comprising a respective voter's vote (v_i) encrypted according to an encryption scheme ($\mathcal{E}_{TM}$); and

a mix-net ($\mathcal{M}$) for decrypting said encrypted votes (v_i) by applying a decryption scheme ($\mathcal{D}_{TM}$) inverse to said encryption scheme ($\mathcal{E}_{TM}$).

18. A computer program having a set of instructions which, when in use on computer apparatus, adapt said computer apparatus so as to constitute a voting system tallier module (50) according to claim 17.